

(11)Publication number : 2001-273133  
(43)Date of publication of application : 05.10.2001

(51)Int.Cl.

G06F 9/06  
G06F 12/14  
G06F 13/00  
G06F 15/00  
G09C 1/00  
H04L 9/08

(21)Application number : 2000-082770

(71)Applicant : TOYO COMMUN EQUIP CO LTD

(22)Date of filing : 23.03.2000

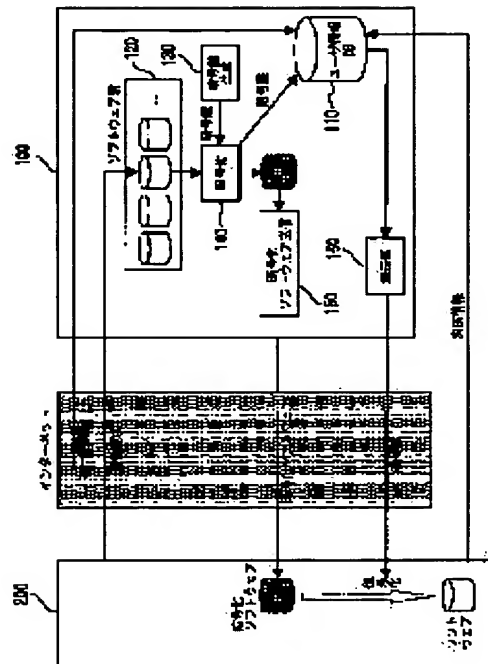
(72)Inventor : NARUSHIMA KOJI

## (54) DEVICE AND METHOD FOR TRANSMITTING SOFTWARE

**(57)Abstract:**

**PROBLEM TO BE SOLVED:** To provide a software transmitter and its method for preventing software from being used by a person who has not made a payment.

**SOLUTION:** This software transmitter 100 for transmitting the software to a user of a terminal device 200 side through the Internet, is provided with a cryptographic key generating part 130 generating a cryptographic key at random each time the user requests software transmission, an enciphering part 140 enciphering the software requested to be transmitted by the generated cryptographic key, an encipherment software transmitting part 150 transmitting the encipherment software that is enciphered to the user requesting its transmission, and a key transmitting part 160 transmitting a decode key corresponding to the cryptographic key with which the software is enciphered to the user when the settlement of the transmitted software is completed.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

**BEST AVAILABLE COPY**

(19)日本国特許庁 (J P)

## (12) 公開特許公報 (A)

(11)特許出願公開番号

特開2001-273133

(P2001-273133A)

(43)公開日 平成13年10月5日(2001.10.5)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	テーマート*(参考)
G 0 6 F 9/06	5 5 0	G 0 6 F 9/06	5 5 0 Z 5 B 0 1 7
12/14	3 2 0	12/14	3 2 0 B 5 B 0 7 6
13/00	5 3 0	13/00	5 3 0 S 5 B 0 8 5
15/00	Z E C	15/00	Z E C 5 J 1 0 4
G 0 9 C 1/00	6 6 0	G 0 9 C 1/00	6 6 0 B 9 A 0 0 1

審査請求 未請求 請求項の数3 O L (全 5 頁) 最終頁に続く

(21)出願番号 特願2000-82770(P2000-82770)

(22)出願日 平成12年3月23日(2000.3.23)

(71)出願人 000003104

東洋通信機株式会社

神奈川県高座郡寒川町小谷2丁目1番1号

(72)発明者 鳴島 康二

神奈川県高座郡寒川町小谷2丁目1番1号

東洋通信機株式会社内

(74)代理人 100098039

弁理士 遠藤 恭

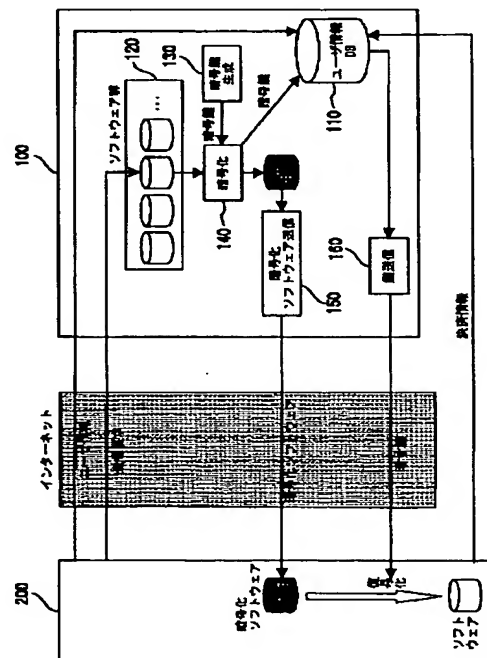
最終頁に続く

(54)【発明の名称】 ソフトウェア送信装置及び方法

## (57)【要約】

【課題】決済を行っていない者によってソフトウェアが使用されることを防止したソフトウェア送信装置及び方法を提供する。

【解決手段】ソフトウェア送信装置100は、インターネットを介して端末装置200側のユーザに対しソフトウェアを送信するものであり、ユーザからソフトウェアの送信要求がされる毎に、ランダムに暗号鍵を生成する暗号鍵生成部130と、生成された暗号鍵によって、送信要求されたソフトウェアを暗号化する暗号化部140と、暗号化された暗号化ソフトウェアを送信を要求したユーザへ送信する暗号化ソフトウェア送信部150と、送信されたソフトウェアに対する決済が完了した場合に、該ソフトウェアを暗号化した暗号鍵に対応する復号鍵をユーザへ送信する鍵送信部160とを備える。



BEST AVAILABLE COPY

## 【特許請求の範囲】

【請求項1】 通信ネットワークを介してユーザに対しソフトウェアを送信するソフトウェア送信装置であって、

前記ユーザからソフトウェアの送信要求がされる毎に、ランダムに暗号鍵を生成する暗号鍵生成手段と、前記生成された暗号鍵によって、前記送信要求されたソフトウェアを暗号化する暗号化手段と、前記暗号化された暗号化ソフトウェアを前記送信を要求したユーザへ送信するソフトウェア送信手段と、前記送信されたソフトウェアに対する決済が完了した場合に、該ソフトウェアを暗号化した暗号鍵に対応する復号鍵を前記ユーザへ送信する鍵送信手段と、を備えることを特徴とするソフトウェア送信装置。

【請求項2】 前記暗号鍵生成手段によって生成された暗号鍵と、該暗号鍵で暗号化されたソフトウェアの識別情報と、該ソフトウェアの送信を要求したユーザの情報とを関連付けて記憶する記憶手段と、前記送信されたソフトウェアに対する決済が完了した場合に、前記ユーザの情報から該決済に対応するソフトウェアを暗号化した暗号鍵を特定する特定手段と、を更に備えることを特徴とする請求項1に記載のソフトウェア送信装置。

【請求項3】 通信ネットワークを介してユーザに対しソフトウェアを送信するソフトウェア送信方法であって、

前記ユーザからソフトウェアの送信要求がされる毎に、ランダムに暗号鍵を生成する手順と、前記生成された暗号鍵によって、前記送信要求されたソフトウェアを暗号化し、前記暗号化された暗号化ソフトウェアを前記送信を要求したユーザへ送信する手順と、前記送信されたソフトウェアに対する決済が完了した場合に、該ソフトウェアを暗号化した暗号鍵に対応する復号鍵を前記ユーザへ送信する手順と、を備えることを特徴とするソフトウェア送信方法。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】 本発明は、通信ネットワークを介してユーザに対しソフトウェアを送信するソフトウェア送信装置及び方法に関する。

## 【0002】

【従来の技術】 近年、インターネット等の通信ネットワークが様々な方面で活用されている。例えば、ソフトウェア送信装置は、ユーザがインターネット上のサイトからプログラムや音楽ソフト等のソフトウェアをダウンロードして購入することを可能としたものである。

【0003】 図2は、従来のソフトウェア送信装置の構成を示すブロック図である。同図に示すソフトウェア送信装置300は、共通鍵暗号方式によりソフトウェアを

暗号化して送信するものである。販売対象の各ソフトウェアは、予めソフトウェア毎に異なる暗号鍵で暗号化されており、暗号化ソフトウェア群210として格納されている。ソフトウェアの送信時には、ユーザは、端末装置400を使用してインターネット上の販売業者のサイトにアクセスした上で購入を希望するソフトウェアを選択する。この選択情報は、送信要求としてソフトウェア送信装置300に送られる。ソフトウェア送信装置300は、この送信要求に応じて暗号化ソフトウェア群210から要求された暗号化ソフトウェアを選択し、端末装置400へ送信する。

【0004】 その後、ユーザが決済を行って、ソフトウェア送信装置300にその決済情報が入力されると、ソフトウェア送信装置300は、送信した暗号化ソフトウェアの暗号化に用いた暗号鍵を端末装置400へ送信する。端末装置400は、この暗号鍵を用いて送信された暗号化ソフトウェアを復号化し、ソフトウェアを使用可能にする。

【0005】 このようにソフトウェア送信装置300では、ユーザが決済を行った場合にのみ、暗号化ソフトウェアを復号化することができる。

## 【0006】

【発明が解決しようとする課題】 しかしながら、上述したソフトウェア送信装置300では、ソフトウェア毎に異なる暗号鍵で暗号化されており、ソフトウェアと暗号鍵とが1対1に対応している。このため、第三者がユーザから暗号鍵を入手した場合には、その第三者は、暗号化ソフトウェアをダウンロードして、入手した暗号鍵で復号化することにより、決済を行うことなくソフトウェアを使用することができてしまう。このような問題を解消すべく、決済を行っていない者によってソフトウェアが使用されることを防止することが要求されている。

【0007】 本発明は、上記従来の問題点を解決するものであり、その目的は、決済を行っていない者によってソフトウェアが使用されることを防止したソフトウェア送信装置及び方法を提供することにある。

## 【0008】

【課題を解決するための手段】 上記目的を達成するため、本発明のソフトウェア送信装置は、通信ネットワークを介してユーザに対しソフトウェアを送信するものであり、前記ユーザからソフトウェアの送信要求がされる毎に、ランダムに暗号鍵を生成する暗号鍵生成手段と、前記生成された暗号鍵によって、前記送信要求されたソフトウェアを暗号化する暗号化手段と、前記暗号化された暗号化ソフトウェアを前記送信を要求したユーザへ送信するソフトウェア送信手段と、前記送信されたソフトウェアに対する決済が完了した場合に、該ソフトウェアを暗号化した暗号鍵に対応する復号鍵を前記ユーザへ送信する鍵送信手段とを備えて構成される。

【0009】 この場合において、前記暗号鍵生成手段に

10

20

30

40

50

よって生成された暗号鍵と、該暗号鍵で暗号化されたソフトウェアの識別情報と、該ソフトウェアの送信を要求したユーザの情報とを関連付けて記憶する記憶手段と、前記送信されたソフトウェアに対する決済が完了した場合に、前記ユーザの情報から該決済に対応するソフトウェアを暗号化した暗号鍵を特定する特定手段とを更に備えることが好ましい。

【0010】また、本発明のソフトウェア送信方法は、通信ネットワークを介してユーザに対しソフトウェアを送信するものであり、前記ユーザからソフトウェアの送信要求がされる毎に、ランダムに暗号鍵を生成する手順と、前記生成された暗号鍵によって、前記送信要求されたソフトウェアを暗号化する手順と、前記暗号化された暗号化ソフトウェアを前記送信を要求したユーザへ送信する手順と、前記送信されたソフトウェアに対する決済が完了した場合に、該ソフトウェアを暗号化した暗号鍵に対応する復号鍵を前記ユーザへ送信する手順とを備えて構成される。

【0011】

【発明の実施の形態】以下、図示した一実施形態に基いて本発明を詳細に説明する。図1は、本発明に係るソフトウェア送信装置の構成を示すブロック図である。同図に示すソフトウェア送信装置100は、インターネットを介して、ユーザが使用する端末装置200と接続されており、ソフトウェア販売業者のサイトのサーバとして機能する。このソフトウェア送信装置100は、暗号鍵と復号鍵が同一である共通鍵暗号方式によりソフトウェアを暗号化して端末装置200へ送信するものであり、ユーザ情報データベース(DB)110、ソフトウェア群120、暗号鍵生成部130、暗号化部140、暗号化ソフトウェア送信部150及び鍵送信部160を含んで構成される。

【0012】端末装置200側のユーザは、ソフトウェアの入手に先立って、予めソフトウェア送信装置100にユーザ登録を行う。具体的には、ユーザは、端末装置200を使用して販売業者のサイトにアクセスした上で、住所、氏名等のユーザ情報を入力する。入力されたユーザ情報は、端末装置200からソフトウェア送信装置100へ送られ、ユーザ情報DB110に格納される。

【0013】このような手順によってユーザ登録が行われると、次に、ユーザは、購入を希望するソフトウェアを選択する。この選択情報は、送信要求としてソフトウェア送信装置100に送られる。

【0014】ソフトウェア群120には、販売される各種のソフトウェアが格納されている。ソフトウェア送信装置100は、ユーザから送信要求が送られると、ソフトウェア群120の中から送信要求されたソフトウェア、すなわちユーザが購入を希望するソフトウェアを選択する。

【0015】暗号鍵生成部130は、ユーザから送信要求が送られ、ソフトウェア群120の中からソフトウェアが選択される毎に、例えば乱数を使用してランダムに暗号鍵を生成する。

【0016】暗号化部140は、暗号鍵生成部130によって生成された暗号鍵を用いて、ソフトウェア群120の中から選択されたソフトウェアを暗号化する。暗号化ソフトウェア送信部150は、暗号化部140によって暗号化されたソフトウェア(暗号化ソフトウェア)を端末装置200へ送信する。また、ソフトウェア送信装置100は、送信されたソフトウェアの識別情報(例えばソフトウェアの名称)と、そのソフトウェアの暗号化に用いられた暗号鍵と、該ソフトウェアの送信を要求したユーザのユーザ情報とを関連付けてユーザ情報DB110に格納する。

【0017】その後、ユーザが端末装置200を使用して販売業者のサイトにアクセスした上で、住所、氏名等のユーザの識別に必要な情報、送信されたソフトウェアの識別情報、クレジットカード番号等を入力して決済を行うと、これらの情報が決済情報として端末装置200からソフトウェア送信装置100へ送られる。なお、決済方法とソフトウェア配信装置100への決済情報の入力方法は上記以外にも考えられ、例えば、ユーザが販売業者の口座に入金することによって決済を行い、ソフトウェア送信装置100の操作者がその入金情報に基づいて決済情報を入力するようにしてもよい。

【0018】ソフトウェア送信装置100は、入力された決済情報をユーザ情報DB110に格納する。また、ソフトウェア送信装置100は、この決済情報に基づいて、決済を行ったユーザと該決済に対応するソフトウェアとを特定する。鍵送信部160は、このように特定された、決済を行ったユーザと該決済に対応するソフトウェアとに関連付けられた暗号鍵を、ユーザ情報DB110から読み出して端末装置200へ送信する。

【0019】端末装置200は、ユーザの復号化指示に応じて、送信された暗号鍵を用いて暗号化ソフトウェアを復号化し、ソフトウェアを使用可能にする。

【0020】このように、ソフトウェア送信装置100は、ユーザからソフトウェアの送信が要求される毎にランダムに暗号鍵を生成し、該暗号鍵を用いてソフトウェアを暗号化して送信し、その後ユーザが決済を行った場合には、その暗号化に用いた暗号鍵を送信する。このため、暗号化ソフトウェアの送信動作と暗号鍵とが1対1に対応することになり、第三者がユーザから暗号鍵を入手すると共に暗号化ソフトウェアをダウンロードしても、入手した暗号鍵で暗号化ソフトウェアを復号化することはできない。従って、決済を行っていない者によってソフトウェアが使用されることを防止することができる。

【0021】以上、本発明の一実施形態を図面に沿って

10

20

30

40

50

説明した。しかしながら本発明は前記実施形態に示した事項に限定されず、特許請求の範囲の記載に基づいてその変更、改良等が可能であることは明らかである。例えば上述した実施形態では、暗号鍵と復号鍵が同一である共通鍵暗号方式が用いられたが、これら暗号鍵と復号鍵は異なってもよい。この場合には、ユーザがソフトウェアに対する決済を行った際に、そのソフトウェアを暗号化した暗号鍵に対応する復号鍵を送信する。また、上述した実施形態では、ソフトウェア送信装置と端末装置とはインターネットによって接続されていたが、他の通信ネットワークによって接続されるようにしてもよい。

【0022】

【発明の効果】以上の如く本発明によれば、ユーザからソフトウェアの送信が要求される毎にランダムに暗号鍵を生成することによって、決済を行っていない者によっ

\*てソフトウェアが使用されることを防止することができる。

【図面の簡単な説明】

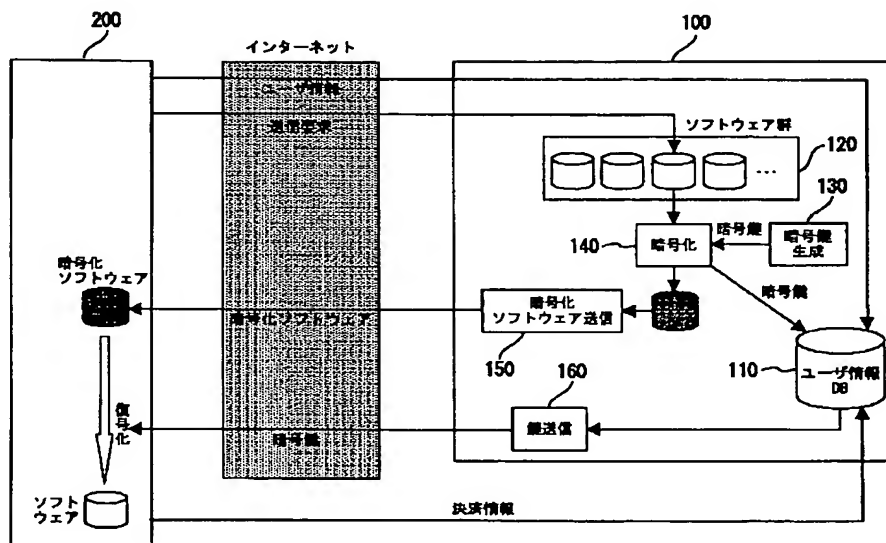
【図1】本発明に係るソフトウェア送信装置の構成を示すブロック図である。

【図2】従来のソフトウェア送信装置の構成を示すブロック図である。

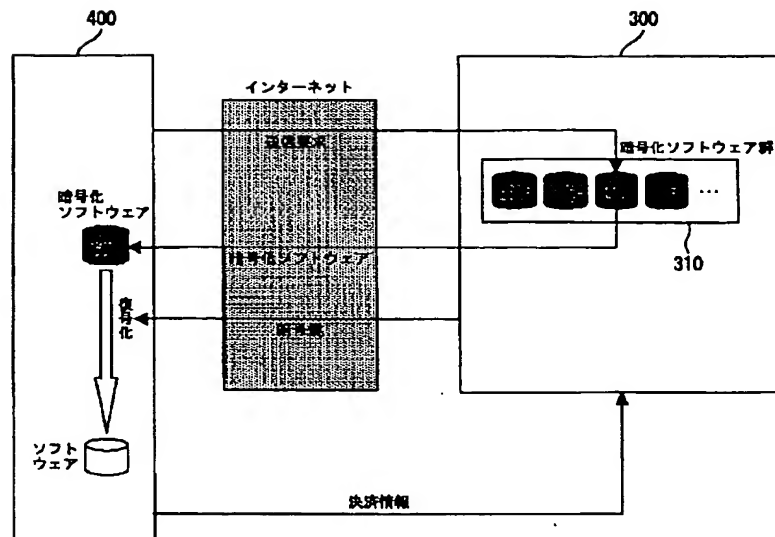
【符号の説明】

100 ソフトウェア送信装置  
110 ユーザ情報DB  
120 ソフトウェア群  
130 暗号鍵生成部  
140 暗号化部  
150 暗号化ソフトウェア送信部  
160 鍵送信部  
200 端末装置

【図1】



【図2】



フロントページの続き

(51)Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード (参考)
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 B

F ターム(参考)

5B017	AA07	BA07	CA15
5B076	FA00	FB01	
5B085	AC04	AE13	AE29
5J104	AA01	AA16	EA01 EA04 EA16
	JA03	NA02	PA07 PA10
9A001	BB04	CC03	EE03 JJ25 KK56
	KK60	LL03	